

Implémentation et vérification du protocole POAP sur la plate-forme Nexus 9000

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Topologie](#)

[Informations générales](#)

[Provisionnement manuel et POAP](#)

[Workflow POAP de haut niveau](#)

[Architecture et workflow POAP](#)

[Phase De Mise Sous Tension](#)

[Phase de découverte USB](#)

[Phase de découverte DHCP](#)

[Échange DHCP](#)

[Informations obtenues via DHCP](#)

[Bail DHCP et validation des offres](#)

[Identification du périphérique POAP](#)

[Récupération de script POAP](#)

[Intégrité des scripts POAP](#)

[Phase d'exécution du script](#)

[Traitement des images logicielles](#)

[Phase de rechargement post-installation](#)

[Réexécution de configuration](#)

[Exigences POAP](#)

[Configurer le POAP](#)

[Exigences d'infrastructure de provisionnement](#)

[Préparation du script POAP](#)

[Configurer l'identification des périphériques](#)

[Exemple de logique de provisionnement](#)

[Préparation de la configuration du périphérique](#)

[Examen D'Accès Administratif](#)

[Préparer les informations d'intégrité des fichiers](#)

[Mettre à jour le script POAP MD5](#)

[Préparation du fichier de configuration MD5](#)

[Préparation de l'image MD5 de Cisco NX-OS](#)

[Démarrer le POAP](#)

[Supprimer la configuration initiale](#)

[Recharger le commutateur](#)

[Initialisation POAP](#)

[Obtenir des informations réseau Bootstrap](#)

[Télécharger et démarrer le script POAP](#)

[Vérifier](#)

[Vérification de l'initialisation POAP](#)

[Vérification des fichiers journaux POAP](#)

[Vérification de la détection DHCP](#)

[Vérification de l'échange DHCP](#)

[Vérification de DHCP avec une capture de paquets](#)

[Vérification de la récupération des scripts POAP](#)

[Vérification de la récupération des scripts avec une capture de paquets](#)

[Vérification de l'intégrité du script POAP](#)

[Vérification de la récupération de la configuration spécifique au périphérique](#)

[Vérification de la récupération des fichiers de configuration](#)

[Vérification de la récupération de configuration avec une capture de paquets](#)

[Vérifier l'intégrité de configuration](#)

[Vérification du traitement de configuration](#)

[Vérification du traitement des images](#)

[Vérification de la récupération MD5 de l'image](#)

[Vérification du workflow d'installation du logiciel](#)

[Vérifier la relecture de configuration](#)

[Vérification de la relecture de la configuration ASCII](#)

[Vérifier la fin du POAP](#)

[Vérification de la configuration provisionnée](#)

[Conclusion](#)

Introduction

Ce document décrit le POAP (PowerOn Auto Provisioning) sur les commutateurs Cisco Nexus 9000 exécutant Cisco NX-OS.

Conditions préalables

Exigences

Cisco vous recommande d'avoir des connaissances de base sur les sujets suivants :

- Interface de ligne de commande (CLI) de Cisco NX-OS
- Adressage IPv4 (Internet Protocol version 4) de base et connectivité de couche 3

- Principes fondamentaux du protocole DHCP (Dynamic Host Configuration Protocol)
- Concepts de base des protocoles HTTP (Hypertext Transfer Protocol) et TFTP (Trivial File Transfer Protocol)

Composants utilisés

Composante	Plate-forme/Logiciels	Version / Valeur	Objectif
Commutateur Nexus	N9K-C9336C-FX2	NX-OS 10.6(2)	périphérique POAP
Serveur de provisionnement	Serveur Ubuntu	24.04.5 LTS	Infrastructure de provisionnement externe
Service DHCP/TFTP	dnsmasq	2.91	Fournit des services DHCP et TFTP

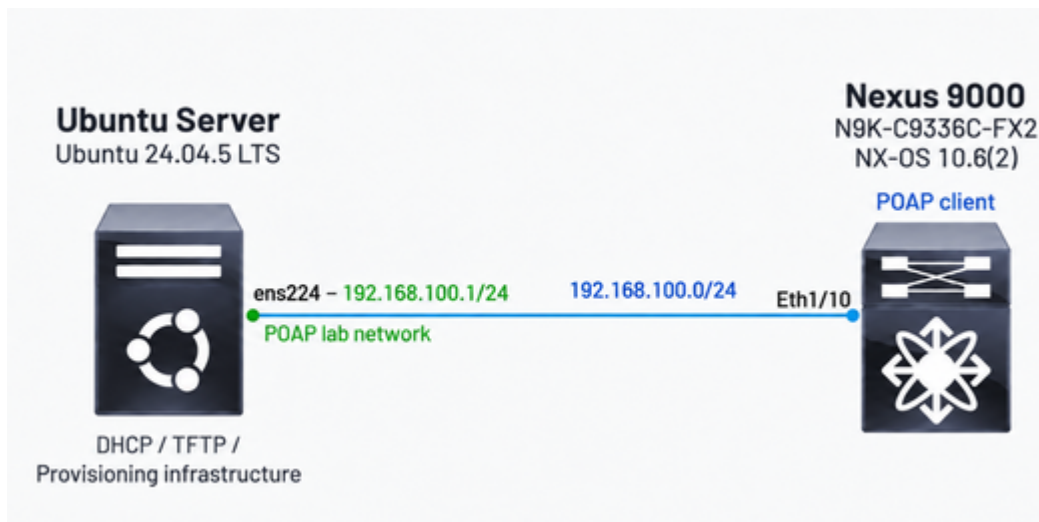
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Topologie

Ces travaux pratiques utilisent un commutateur Cisco Nexus 9000 connecté directement à un serveur Ubuntu qui fournit l'infrastructure de mise en service externe.

L'objectif est de conserver une topologie simple afin que le flux de travail POAP puisse être observé sans périphériques réseau supplémentaires entre le commutateur Nexus et le serveur de mise en service.

Ethernet1/10 sur le commutateur Nexus est connecté directement à ens224 sur le serveur Ubuntu.



Informations générales

Le déploiement d'un nouveau commutateur Cisco Nexus nécessite une configuration initiale avant que le périphérique puisse participer au réseau.

PowerOn Auto Provisioning (POAP) automatise ce processus d'amorçage. Lorsqu'un commutateur Nexus pris en charge démarre sans configuration initiale, Cisco NX-OS peut passer en mode POAP, obtenir des informations réseau temporaires via DHCP, récupérer un script d'approvisionnement et utiliser ce script afin d'approvisionner l'image logicielle et la configuration de périphérique requises.

Le protocole POAP est principalement associé au provisionnement initial, ou au jour 0, car le commutateur peut obtenir les ressources nécessaires au déploiement sans avoir à saisir manuellement la configuration complète via l'interface de ligne de commande.

Provisionnement manuel et POAP

Sans POAP, le déploiement initial d'un commutateur Nexus peut nécessiter une interaction manuelle afin de configurer la connectivité réseau, transférer les fichiers de configuration et préparer l'image logicielle Cisco NX-OS requise.

Avec le protocole POAP, le commutateur peut détecter automatiquement l'infrastructure de provisionnement et récupérer les ressources nécessaires au déploiement.

Workflow POAP de haut niveau

À un niveau élevé, le POAP commence lorsqu'un commutateur Nexus pris en charge démarre sans configuration initiale. Le commutateur démarre le processus de mise à disposition et tente d'obtenir les informations réseau nécessaires pour accéder à l'infrastructure de mise à disposition.

Une fois la connectivité réseau établie, le commutateur récupère et exécute le script POAP. Le script détermine l'image logicielle et les ressources de configuration associées au périphérique et contrôle les opérations de mise en service restantes.

Cisco définit le processus POAP en cinq phases principales :

- Mise sous tension
- Détection USB
- Détection DHCP
- Exécution du script
- Rechargement post-installation

La section suivante décrit le rôle de chaque phase au cours du processus de provisionnement.

Architecture et workflow POAP

POAP fonctionne comme un processus d'amorçage intermédiaire dans Cisco NX-OS. Chaque phase exécute une fonction spécifique requise pour la mise en service automatique des périphériques.

La compréhension de ces phases fournit la base du workflow de mise en oeuvre et de vérification décrit plus loin dans ce document.

Phase De Mise Sous Tension

Lorsqu'un commutateur Nexus est mis sous tension, Cisco NX-OS charge l'image du logiciel installé et recherche une configuration initiale.

Si une configuration initiale existe, le commutateur poursuit le processus de démarrage normal. Si aucune configuration initiale n'est trouvée, le mode POAP démarre.

Au démarrage, NX-OS affiche une invite qui permet d'abandonner le POAP et de poursuivre la configuration interactive normale. Le POAP continue sans intervention de l'utilisateur.

Si le POAP continue, les interfaces du panneau avant sont placées dans leur configuration par défaut avant le début du processus de détection.

Condition	Résultat
La configuration initiale est présente.	NX-OS poursuit le processus de démarrage normal.
La configuration initiale est absente.	Le mode POAP démarre.
Le POAP est abandonné manuellement.	NX-OS entre dans la configuration interactive normale.
Le POAP continue.	Le processus se poursuit avec la détection USB.

Phase de découverte USB

Une fois le POAP démarré, NX-OS recherche les périphériques USB accessibles pour provisionner les ressources.

Si un script POAP est détecté sur un périphérique USB, NX-OS démarre l'exécution du script. Si aucun script utilisable n'est trouvé, le protocole POAP procède à la détection DHCP.

Le provisionnement basé sur USB fait partie du workflow POAP ; toutefois, la mise en oeuvre dans ce document se concentre sur le provisionnement basé sur le réseau via DHCP.

Phase de découverte DHCP

Si aucun script POAP n'est trouvé pendant la détection USB, le commutateur démarre la détection DHCP.

Au cours de cette phase, le commutateur envoie des messages de détection DHCP via les interfaces disponibles du panneau avant ou l'interface de gestion afin de localiser un serveur DHCP qui peut fournir les informations requises pour le POAP.

Le client DHCP Cisco Nexus utilise le numéro de série du commutateur dans l'identificateur du client. Ces informations peuvent être utilisées par l'infrastructure de mise en service afin d'identifier le périphérique et de fournir les informations d'amorçage requises pour le processus de mise en service.

Échange DHCP

La négociation DHCP utilise le processus standard DORA (Discover, Offer, Request, Acknowledgement) :

Message DHCP	Objectif
Découvrir	Le commutateur Nexus recherche un serveur DHCP disponible.
Offre	Le serveur DHCP fournit des informations relatives au réseau et au POAP.
Demande	Le commutateur demande l'offre DHCP sélectionnée.
Accusé de réception	Le serveur DHCP confirme le bail et attribue l'adresse IP.

Informations obtenues via DHCP

Pour les POAP réseau, l'échange DHCP fournit les informations réseau temporaires et les paramètres d'amorçage nécessaires pour localiser le script POAP.

Le message de détection DHCP demande des informations qui incluent :

- Nom ou adresse du serveur TFTP
- Nom du fichier de démarrage

Le nom du fichier de démarrage identifie le script POAP que le commutateur récupère une fois la négociation DHCP terminée.

DHCP ne fournit pas la configuration finale de Cisco Nexus. Il fournit les informations d'amorçage nécessaires pour établir une connectivité temporaire et localiser le script de mise en service.

Bail DHCP et validation des offres

Le protocole POAP nécessite une période de bail DHCP minimale de 3 600 secondes.

La réception d'une offre DHCP ne signifie pas automatiquement que la découverte DHCP réussit. L'offre doit répondre aux exigences attendues par le POAP avant que le commutateur ne poursuive l'échange de requête et d'accusé de réception DHCP.

Si aucune offre valide n'est reçue, aucune adresse IP n'est attribuée via cette offre.

Identification du périphérique POAP

À partir de la version 7.0(3)I7(4) de Cisco NX-OS, POAP prend en charge l'option de classe d'utilisateur DHCP définie par la RFC 3004.

Pour DHCPv4, le POAP utilise l'option de classe d'utilisateur 77 avec cette valeur : Cisco-POAP

Cette valeur identifie la requête DHCP comme provenant du processus POAP.

La valeur Cisco-POAP peut être observée plus loin dans la capture de paquets utilisée lors de la vérification.

Récupération de script POAP

Une fois la négociation DHCP terminée, le commutateur utilise les informations d'approvisionnement reçues du serveur DHCP afin de localiser et de récupérer le script POAP.

Dans le workflow réseau standard utilisé dans ce document, les informations DHCP identifient le serveur TFTP et le fichier de démarrage qui contient le script de mise en service. Une fois la connectivité réseau temporaire établie, Cisco NX-OS télécharge le script à partir du serveur d'approvisionnement.

Le script POAP contient la logique requise pour déterminer et traiter l'image logicielle et les ressources de configuration associées au périphérique.

Cisco fournit un script POAP de référence écrit en Python. Le script peut être personnalisé afin de correspondre à l'environnement de mise en service.

Intégrité des scripts POAP

Le script POAP de référence Cisco inclut une somme de contrôle MD5.

Lorsque le script est modifié, la somme de contrôle incorporée doit être recalculée avant que le script ne soit utilisé pour le POAP.

La procédure de préparation de la somme de contrôle est décrite plus loin dans la section Préparer les informations d'intégrité de fichier.

Phase d'exécution du script

Une fois le script POAP téléchargé et validé, Cisco NX-OS exécute le script localement sur le commutateur.

Le script de référence peut effectuer des tâches d'approvisionnement telles que :

- Identifiez le commutateur.
- Sélectionnez la configuration spécifique au périphérique.
- Récupérer et valider la configuration.
- Déterminez l'image Cisco NX-OS cible.
- Récupérez ou validez l'image logicielle.
- Préparez la configuration pour la relecture.
- Exécutez le workflow de provisionnement.

La configuration téléchargée n'est pas nécessairement appliquée immédiatement pendant l'exécution du script.

Cisco NX-OS peut préparer la configuration et l'appliquer après le démarrage du commutateur avec l'image logicielle cible. La configuration est donc traitée dans l'environnement logiciel pour lequel elle a été préparée.

Traitement des images logicielles

Le script POAP peut déterminer si l'image Cisco NX-OS cible est déjà disponible localement.

Si l'image requise n'est pas présente, le script peut la récupérer à partir de l'infrastructure de mise en service.

Si l'image requise est déjà disponible, le script peut valider le fichier existant et éviter de télécharger une autre copie.

Dans l'implémentation validée, l'image cible était déjà présente dans bootflash:. Le script a validé l'image avant de poursuivre les opérations de provisionnement restantes.

Phase de rechargement post-installation

Une fois l'exécution du script terminée, le commutateur entre en phase de rechargement post-installation.

Au cours de cette phase, le commutateur redémarre et démarre avec l'image logicielle Cisco NX-OS cible lorsqu'une modification d'image logicielle fait partie du processus de provisionnement.

Le commutateur applique ou lit ensuite la configuration téléchargée. Une fois la configuration correctement appliquée, Cisco NX-OS copie la configuration en cours dans la configuration initiale.

Cette séquence garantit que la configuration provisionnée est traitée dans l'environnement logiciel pour lequel elle a été préparée.

Réexécution de configuration

La relecture de la configuration est le processus par lequel Cisco NX-OS applique la configuration téléchargée pendant le POAP après le redémarrage du commutateur.

Le fichier de configuration n'est pas nécessairement appliqué lors de son téléchargement initial. Au lieu de cela, POAP peut préparer la configuration pendant l'exécution du script et l'appliquer une fois que l'image Cisco NX-OS cible est active.

Le processus peut se résumer comme suit :

Étape	Action
Exécution du script	Récupère l'image logicielle et la configuration requises.
Rechargement post-installation	Redémarre le commutateur après les opérations de provisionnement.
Réexécution de la configuration	Applique la configuration téléchargée.
Persistance de configuration	Copie la configuration en cours dans la configuration initiale.

Cette séparation entre la récupération de la configuration et l'application de configuration est une partie importante du workflow POAP.

Exigences POAP

Le POAP basé sur le réseau nécessite une infrastructure externe afin de fournir une connectivité réseau temporaire et un accès aux ressources de mise en service.

Pour le workflow POAP standard, l'infrastructure requise inclut :

- Serveur DHCP qui fournit les informations réseau requises lors du démarrage.
- Serveur TFTP qui fournit le script POAP.
- Un ou plusieurs serveurs qui fournissent les images logicielles Cisco NX-OS et les fichiers

de configuration des périphériques requis.

Les informations réseau obtenues via DHCP sont utilisées lors du processus de mise en service POAP.

Configurer le POAP

Cette section décrit les composants requis pour mettre en oeuvre le provisionnement automatique PowerOn (POAP) basé sur le réseau sur un commutateur Cisco Nexus 9000.

Le protocole POAP s'appuie sur des services DHCP et de transfert de fichiers externes afin de fournir une connectivité réseau temporaire et un accès aux ressources de mise en service. La configuration de plates-formes de serveurs tiers sort du cadre de ce document.

Les exemples de cette section utilisent la topologie décrite précédemment afin de démontrer l'implémentation POAP.

Exigences d'infrastructure de provisionnement

Pour la mise en oeuvre validée, l'infrastructure de mise en service fournit les informations réseau temporaires et les services de transfert de fichiers requis par le commutateur Nexus pendant le POAP.

L'infrastructure DHCP doit fournir les informations requises afin d'établir une connectivité temporaire et de localiser le script POAP. Le protocole POAP nécessite un bail DHCP d'au moins 3 600 secondes.

Informations	Objectif
Adresse IP	Fournit une connectivité réseau temporaire pendant le POAP.
Subnet Mask (Masque de sous-réseau)	Définit le sous-réseau IP temporaire.
Passerelle par défaut	Fournit la connectivité aux ressources de provisionnement lorsque le routage est requis.
Nom ou adresse du serveur TFTP	Identifie le serveur à partir duquel le script POAP est récupéré.
Nom du fichier de démarrage	Identifie le script POAP que le commutateur Nexus télécharge.

Une fois qu'une offre DHCP valide est sélectionnée, le commutateur Nexus termine la négociation DHCP et utilise les informations réseau attribuées lors du processus de mise en service.

Pour l'exemple validé de ce document, l'infrastructure de provisionnement utilise les valeurs suivantes :

Paramètre	Valeur Lab
réseau POAP	192.168.100.0/24
Serveur de provisionnement	192.168.100.1
Plage d'adresses DHCP	192.168.100.100–192.168.100.110
bail DHCP	2 heures
Serveur TFTP	192.168.100.1
script POAP	poap.py
interface Nexus	Ethernet1/10

Le serveur de mise en service utilisé dans cet exemple exécute Ubuntu et fournit les services DHCP et TFTP requis pour la mise en oeuvre. La configuration détaillée du logiciel de serveur tiers n'est pas traitée dans ce document.

Préparation du script POAP

Cisco fournit un script POAP de référence développé en Python. Modifiez les options modifiables par l'utilisateur afin de correspondre à l'environnement de provisionnement.

Le script POAP agit en tant qu'orchestrateur de mise en service. Une fois que le commutateur Nexus a téléchargé et validé le script, celui-ci détermine comment le commutateur récupère et traite les ressources de configuration et d'image logicielle requises pour le provisionnement.

Pour la mise en oeuvre validée, les options suivantes sont utilisées :

```
options = { "username": "root", "password": "password", "hostname": "192.168.100.1", "transfer_protocol": "tftp", "mode": "serial_number",  
"target_system_image": "nxos64-cs.10.6.2.F.bin", "config_path": "/", "target_image_path": "/", }
```

Les valeurs indiquées dans cet exemple correspondent à l'environnement des travaux pratiques. Les valeurs de production dépendent de l'infrastructure de provisionnement et des exigences de déploiement.

Option	Valeur Lab	Objectif
nom de l'hôte	192.168.100.1	Identifie le serveur à partir duquel les fichiers d'approvisionnement sont récupérés.
protocole_transfert	tftp	Définit le protocole de transfert de fichiers.
mode	numéro_de_série	Utilise le numéro de série du commutateur afin de sélectionner le fichier de configuration spécifique au périphérique.

Option	Valeur Lab	Objectif
image_système_cible	nxos64-cs.10.6.2.F.bin	Définit l'image Cisco NX-OS cible.
chemin_config	/	Définit le chemin qui contient la configuration du périphérique.
chemin_image_cible	/	Définit le chemin qui contient l'image logicielle cible.

Le script de référence requiert un nom d'hôte, un nom d'utilisateur et un mot de passe lorsque des fichiers sont récupérés à partir d'un serveur distant. L'exemple utilise TFTP, qui ne fournit pas l'authentification par nom d'utilisateur et mot de passe ; cependant, le script de référence valide toujours la présence de ces paramètres lors de l'initialisation.

Configurer l'identification des périphériques

La mise en oeuvre validée utilise :

```
"mode": "serial_number"
```

En mode serial_number, le script récupère le numéro de série du commutateur local et l'utilise afin de déterminer le nom de fichier de configuration correspondant.

Exemple :

Numéro de série du commutateur : FDO262921L3

Fichier de configuration : conf.FDO262921L3

Le nom du fichier de configuration utilise le format suivant : conf.<numéro-de-série>

Le même script poap.py peut donc prendre en charge plusieurs commutateurs Nexus tandis que chaque commutateur récupère sa propre configuration spécifique au périphérique.

Exemple de logique de provisionnement

À un niveau élevé, le script validé exécute cette séquence :

Identify the switch. ↓ Select conf.

. ↓ Retrieve and validate the configuration. ↓ Determine the target Cisco NX-OS image. ↓ Validate or retrieve the image. ↓ Prepare the

configuration for replay. ↓ Complete the provisioning workflow.

Le script POAP ne contient pas la configuration complète du périphérique. Il contient la logique et les paramètres requis pour localiser, valider et traiter les ressources de mise en service.

Préparation de la configuration du périphérique

Le fichier de configuration du périphérique contient la configuration Cisco NX-OS que le POAP provisionne sur le commutateur Nexus cible.

Pour le commutateur utilisé dans cet exemple, le mode `serial_number` sélectionne ce fichier de configuration :

Numéro de série: FDO262921L3

Fichier de configuration : `conf.FDO262921L3`

Le fichier de configuration contient les commandes requises pour établir la configuration Day-0 prévue.

Pour l'implémentation validée, la configuration contient un utilisateur administratif, un nom d'hôte et une interface de bouclage :

```
username admin password
```

```
role network-admin hostname N9K-POAP-SW1 interface loopback100 description POAP-VALIDATION ip address 10.255.255.100/32 no shutdown
```

La configuration est intentionnellement minimale afin de simplifier la vérification du workflow de mise en service.

Une fois le POAP terminé, le nom d'hôte, le compte d'administration et l'interface Loopback100 fournissent des indicateurs clairs indiquant que la configuration spécifique au périphérique a été correctement appliquée.

Examen D'Accès Administratif

La configuration provisionnée doit inclure l'accès administratif requis une fois le POAP terminé.



Mise en garde : Assurez-vous que la configuration du périphérique contient un mot de passe et un utilisateur administratif valides. Le POAP peut s'exécuter correctement même si la configuration provisionnée ne fournit pas d'accès administratif valide.

Lors de la validation initiale des travaux pratiques, la configuration du périphérique contenait le nom d'hôte et l'interface Loopback100, mais ne contenait pas d'utilisateur administratif. POAP terminé avec succès ; toutefois, l'accès administratif n'était pas disponible après le provisionnement.

L'achèvement du POAP confirme que le workflow de mise en service s'est terminé correctement. Il ne confirme pas que la configuration Day-0 contient tous les paramètres requis pour fonctionner et accéder au commutateur.

Préparer les informations d'intégrité des fichiers

Le workflow POAP de référence utilise des sommes de contrôle MD5 afin de vérifier l'intégrité des ressources de provisionnement avant le traitement par le commutateur Nexus.

Le protocole POAP compare la somme de contrôle attendue à la somme de contrôle calculée à partir du fichier correspondant. Les valeurs correspondantes confirment que le fichier contient les données attendues.

La mise en oeuvre validée utilise des informations d'intégrité pour ces ressources :

Ressource	Information D'Intégrité	Objectif
script POAP	Valeur MD5 incorporée dans poap.py	Valide le script avant son exécution.
Configuration de périphériques	conf.FDO262921L3.md5	Valide la configuration de périphérique téléchargée.
Image Cisco NX-OS	nxos64-cs.10.6.2.F.bin.md5	Valide l'image logicielle cible.

L'option `disable_md5` du script de référence contrôle la validation MD5. La valeur par défaut est `False`.

Mettre à jour le script POAP MD5

Le script POAP de référence contient une valeur MD5 près du début du fichier :

```
#md5sum=""
```

```
"
```

Une fois le contenu du script modifié, la somme de contrôle incorporée doit être recalculée avant que le script ne soit utilisé pour le POAP.

Pour le script utilisé dans cette implémentation, la somme de contrôle a été mise à jour avec :

```
f=poap.py cat "$f" | sed '/^#md5sum/d' > "$f.md5" sed -i "s/^#md5sum=.*/#md5sum=\"$(md5sum "$f.md5" | sed 's/./\n/g')\"/" "$f" rm -f "$f.md5"
```

Le script résultant contenait :

```
#md5sum="e4dd91fd4296d40abd2f6187152cd86e"
```

Au cours du POAP, Cisco NX-OS calcule la somme de contrôle du script téléchargé et la compare à la valeur incorporée avant l'exécution du script.

Préparation du fichier de configuration MD5

Le script de référence peut utiliser un fichier MD5 séparé afin de vérifier la configuration du périphérique.

Pour cette mise en oeuvre :

Fichier de configuration :

conf.FDO262921L3

Fichier d'intégrité :

conf.FDO262921L3.md5

Le fichier d'intégrité doit contenir la somme de contrôle associée à la version actuelle de conf.FDO262921L3.

Une fois la configuration téléchargée, le script calcule sa somme de contrôle et la compare à la valeur attendue avant le traitement de la configuration.

Si la configuration du périphérique change, mettez à jour les informations MD5 correspondantes avant la prochaine tentative POAP.

Préparation de l'image MD5 de Cisco NX-OS

Le script de référence peut également valider l'image Cisco NX-OS cible.

Pour cette mise en oeuvre :

Image cible :

nxos64-cs.10.6.2.F.bin

Fichier d'intégrité :

nxos64-cs.10.6.2.F.bin.md5

Le fichier d'intégrité contient :

```
ce50c3f0e387bee578e615a373a4ede0 nxos64-cs.10.6.2.F.bin
```

Dans l'implémentation validée, l'image cible était déjà présente dans bootflash:. Le script POAP a calculé la somme de contrôle MD5 de l'image existante et l'a comparée à la valeur obtenue à partir du serveur d'approvisionnement.

Les deux valeurs correspondant, le fichier image n'a pas besoin d'être téléchargé à nouveau.



Remarque : La validation MD5 vérifie l'intégrité des fichiers. Il ne chiffre pas les fichiers d'approvisionnement et ne fournit pas l'authentification par lui-même.

Démarrer le POAP

Le POAP s'exécute pendant le démarrage du système lorsque le commutateur n'a pas de configuration de démarrage et que le POAP à l'échelle du système est activé.

Avant de démarrer le processus de provisionnement, vérifiez l'état POAP :

```
N9K-POAP-SW1# show system poap System-wide POAP is enabled
```

Cisco NX-OS permet la désactivation globale du POAP avec le système sans POAP. Afin d'activer à nouveau POAP, utilisez `system poap` ou effacez l'indicateur de désactivation POAP avec `write erase poap`.

Supprimer la configuration initiale

Le POAP standard démarre lorsque le commutateur démarre sans configuration initiale.

Dans un environnement de travaux pratiques contrôlé, exécutez :

```
switch# write erase
```



Avertissement : Cette commande efface la configuration de démarrage.

```
Do you wish to proceed anyway? (y/n) [n] y
```

L'opération d'effacement d'écriture par défaut supprime la configuration initiale de la mémoire persistante. Il n'efface pas la configuration en cours ou les variables de démarrage.

Vérifiez que la configuration initiale n'est plus présente :

```
switch# show startup-config No startup configuration
```



Mise en garde : write erase supprime la configuration de commutateur enregistrée. Utilisez cette procédure uniquement lorsque la configuration peut être supprimée ou restaurée en toute sécurité.

Afin d'éviter de perdre l'accès administratif après le POAP, assurez-vous que la configuration de périphérique préparée dans la section précédente contient les informations d'identification administratives requises.

Recharger le commutateur

Une fois la configuration initiale supprimée, rechargez le commutateur.

Si Cisco NX-OS vous invite à enregistrer la configuration en cours, ne l'enregistrez pas. L'enregistrement de la configuration en cours recrée la configuration initiale et empêche la condition de déclenchement POAP standard.

Au démarrage, Cisco NX-OS initialise le protocole POAP et fournit une option permettant d'abandonner le processus :

Abort Power On Auto Provisioning [yes - continue with normal setup, no - continue with Power On Auto Provisioning] (yes/no)[no]:

Afin de continuer avec POAP, acceptez l'option no par défaut.

Initialisation POAP

Une fois le POAP initialisé, le commutateur vérifie d'abord les ressources de mise en service basées sur USB. Si aucun script de mise en service USB utilisable n'est trouvé, le protocole POAP procède à une détection basée sur le réseau.

L'implémentation validée a généré les messages suivants :

```
2026 Sep 22 18:21:23 switch %$ VDC-1 %$ %POAP-2-POAP_INITED: [FDO262921L3-88:FC:5D:BA:D7:7F] - POAP process initialized
2026 Sep 22 18:21:41 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F] - USB Initializing Success 2026
Sep 22 18:21:41 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F] - USB disk not detected
```

Le POAP démarre ensuite la découverte DHCP IPv4 :

2026 Sep 22 18:23:54 switch %\$ VDC-1 %\$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F] - Start DHCP v4 session 2026
Sep 22 18:23:54 switch %\$ VDC-1 %\$ %POAP-2-POAP_DHCP_DISCOVER_START: [FDO262921L3-88:FC:5D:BA:D7:7F] - POAP DHCP
Discover phase started

Obtenir des informations réseau Bootstrap

Une fois qu'une réponse DHCP valide a été reçue, Cisco NX-OS affiche les paramètres réseau temporaires et l'emplacement du script POAP.

La mise en oeuvre validée a produit :

2026 Sep 22 18:23:58 switch %\$ VDC-1 %\$ %POAP-2-POAP_INFO: Recieved DHCP offer from server ip - 192.168.100.1 2026 Sep 22
18:24:02 switch %\$ VDC-1 %\$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F] - Using DHCP, valid information received
over Eth1/10 from 192.168.100.1 2026 Sep 22 18:24:02 switch %\$ VDC-1 %\$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F]
- Assigned IP address: 192.168.100.108 2026 Sep 22 18:24:02 switch %\$ VDC-1 %\$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F]
- Netmask: 255.255.255.0 2026 Sep 22 18:24:02 switch %\$ VDC-1 %\$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F]
- Default Gateway: 192.168.100.1 2026 Sep 22 18:24:02 switch %\$ VDC-1 %\$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F]
- Script Server: 192.168.100.1 2026 Sep 22 18:24:02 switch %\$ VDC-1 %\$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F]
- Script Name: poap.py

À ce stade, la détection DHCP est terminée. Le commutateur dispose d'une connectivité réseau temporaire et des informations requises pour localiser le script POAP.

Télécharger et démarrer le script POAP

Le commutateur récupère le script POAP identifié lors de la détection DHCP :

2026 Sep 22 18:24:14 switch %\$ VDC-1 %\$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F] - The POAP Script download has
started 2026 Sep 22 18:24:14 switch %\$ VDC-1 %\$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F] - The POAP Script is
being downloaded from [copy tftp://192.168.100.1/poap.py bootflash:scripts/script.sh vrf default] 2026 Sep 22 18:24:15 switch %\$ VDC-1 %\$
%POAP-2-POAP_SCRIPT_DOWNLOADED: [FDO262921L3-88:FC:5D:BA:D7:7F] - Successfully downloaded POAP script file

Une fois la récupération du script terminée, le protocole POAP procède à la validation et à

l'exécution du script. Le script de référence contrôle ensuite l'identification du périphérique, la récupération de la configuration, le traitement de l'image logicielle, le transfert de la configuration et les opérations de mise en service restantes.

Vérifier

Utilisez les informations de cette section afin de vérifier chaque étape principale du flux de travail POAP.

Le POAP peut être vérifié de plusieurs points de vue. La console Nexus et les journaux POAP fournissent des informations sur le processus de provisionnement interne, tandis que les journaux du serveur DHCP et les captures de paquets offrent une visibilité supplémentaire sur les échanges réseau.

La mise en oeuvre validée utilise ces sources afin de corréliser le workflow de provisionnement :

Source de vérification	Informations fournies
console Nexus	Initialisation POAP, découverte DHCP, exécution de script, rechargement et relecture de configuration
Journaux POAP Nexus	Informations détaillées sur l'initialisation et l'exécution des scripts
Journaux du serveur DHCP	Négociation DHCP et activité de transfert de fichiers
Capture de paquets	Échanges DHCP et TFTP
Configuration en cours et de démarrage	Résultat final du provisionnement



Remarque : Les résultats de cette section ont été collectés lors des tentatives de validation POAP contrôlées. Une tentative ultérieure a été utilisée afin de valider la configuration finale du jour 0 avec un accès administratif. Les horodatages et les messages de journal d'origine sont conservés dans les exemples.

Les journaux de serveur tiers et les captures de paquets sont inclus uniquement en tant que sources de vérification supplémentaires. La configuration de logiciels tiers sort du cadre de ce document.

Vérification de l'initialisation POAP

Au démarrage du système, vérifiez que le protocole POAP s'initialise correctement.

La console Nexus affiche l'événement d'initialisation :

```
2026 Sep 22 18:21:23 switch %$ VDC-1 %$ %POAP-2-POAP_INITED: [FDO262921L3-88:FC:5D:BA:D7:7F] - POAP process initialized
```

Ce message confirme que le commutateur est entré dans le workflow POAP.

Le POAP recherche ensuite les ressources de mise en service basées sur USB :

```
2026 Sep 22 18:21:41 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F] - USB Initializing Success 2026
Sep 22 18:21:41 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F] - USB disk not detected
```

Dans cet exemple, aucune ressource de mise en service USB n'est disponible. Le protocole POAP continue donc avec la découverte basée sur le réseau.

Le commutateur démarre ensuite la détection DHCP :

```
2026 Sep 22 18:23:54 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F] - Start DHCP v4 session 2026
Sep 22 18:23:54 switch %$ VDC-1 %$ %POAP-2-POAP_DHCP_DISCOVER_START: [FDO262921L3-88:FC:5D:BA:D7:7F] - POAP DHCP
Discover phase started
```

Ces messages confirment la transition de la détection USB à la détection DHCP basée sur le réseau.

Vérification des fichiers journaux POAP

POAP stocke les journaux d'initialisation et d'exécution de script dans bootflash:. Ces fichiers fournissent des informations supplémentaires sur le processus de mise en service après la génération des événements de console.

```
N9K-POAP-SW1# dir bootflash: | include poap 5664 Sep 22 19:52:10 2026 20260922195156_poap_24710_script.log 87366 Sep 22 19:58:48
2026 20260922_194902_poap_24710_init.log N9K-POAP-SW1#
```

Le fichier _init.log contient des informations relatives à l'initialisation et à la découverte POAP.

Le fichier _script.log contient des informations détaillées générées lors de l'exécution du script POAP.

Lorsque plusieurs tentatives POAP existent, utilisez l'horodatage dans le nom de fichier afin de corréler chaque fichier avec la tentative de mise en service correspondante.

Vérification de la détection DHCP

Une fois que le POAP est entré dans la phase de découverte DHCP, vérifiez que le commutateur Nexus reçoit des informations de réseau bootstrap valides.

La console Nexus confirme que la détection DHCP a démarré et que des informations valides ont été reçues via Ethernet1/10 :

```
2026 Sep 22 18:23:54 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F] - Start DHCP v4 session 2026
Sep 22 18:23:54 switch %$ VDC-1 %$ %POAP-2-POAP_DHCP_DISCOVER_START: [FDO262921L3-88:FC:5D:BA:D7:7F] - POAP DHCP
Discover phase started 2026 Sep 22 18:23:58 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: Recieved DHCP offer from server ip -
192.168.100.1 2026 Sep 22 18:24:02 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F] - Using DHCP,
valid information received over Eth1/10 from 192.168.100.1 2026 Sep 22 18:24:02 switch %$ VDC-1 %$ %POAP-2-POAP_INFO:
[FDO262921L3-88:FC:5D:BA:D7:7F] - Assigned IP address: 192.168.100.108 2026 Sep 22 18:24:02 switch %$ VDC-1 %$ %POAP-2-
POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F] - Netmask: 255.255.255.0 2026 Sep 22 18:24:02 switch %$ VDC-1 %$ %POAP-2-
POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F] - Default Gateway: 192.168.100.1 2026 Sep 22 18:24:02 switch %$ VDC-1 %$ %POAP-
2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F] - Script Server: 192.168.100.1 2026 Sep 22 18:24:02 switch %$ VDC-1 %$ %POAP-2-
POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F] - Script Name: poap.py
```

Le résultat confirme que le protocole POAP a sélectionné Ethernet1/10, a obtenu l'adresse temporaire 192.168.100.108 et a reçu la passerelle, le serveur de script et le nom de fichier de script requis pour la prochaine étape d'approvisionnement.

Vérification de l'échange DHCP

Les journaux du serveur DHCP fournissent une vue supplémentaire de l'échange des données d'amorçage.

L'exemple validé enregistré :

```
vendor class: Cisco N9K-C9336C-FX2 user class: Cisco-POAP DHCPDISCOVER(ens224) 88:fc:5d:ba:d7:7f DHCPOFFER(ens224)
```

192.168.100.108 88:fc:5d:ba:d7:7f DHCPREQUEST(ens224) 192.168.100.108 88:fc:5d:ba:d7:7f DHCPACK(ens224) 192.168.100.108 88:fc:5d:ba:d7:7f

Le serveur a également identifié les informations d'amorçage POAP :

option: 67 bootfile-name poap.py option:150 tftp-server-address 192.168.100.1 option: 3 router 192.168.100.1

Les journaux confirment l'intégralité de l'échange Découverte, Offre, Demande et Accusé de réception. Les journaux indiquent également la classe d'utilisateur Cisco-POAP, le nom de fichier de script, l'adresse du serveur TFTP et la passerelle par défaut associés à la demande de mise en service.

Vérification de DHCP avec une capture de paquets

Une capture de paquets peut être utilisée afin de vérifier l'échange DHCP directement sur le réseau.

Pour l'exemple validé, la capture a été examinée avec :

```
sudo tcpdump -nn -vvv -r /tmp/poap-run1.pcap \ 'udp port 67 or udp port 68'
```

La capture montrait :

DHCP-Message (53), length 1: Discover Vendor-Class (60), length 20: "Cisco N9K-C9336C-FX2" DHCP-Message (53), length 1: Offer
DHCP-Message (53), length 1: Request Requested-IP (50), length 4: 192.168.100.108 DHCP-Message (53), length 1: ACK

La capture de paquets confirme la séquence de détection, d'offre, de demande et d'accusé de réception observée dans les journaux du serveur DHCP.

Vérification de la récupération des scripts POAP

Une fois la détection DHCP terminée, vérifiez que le commutateur Nexus récupère le script POAP à partir du serveur identifié lors de l'échange DHCP.

La console Nexus indique le début du téléchargement du script :

```
2026 Sep 22 18:24:14 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F] - The POAP Script download has
started 2026 Sep 22 18:24:14 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F] - The POAP Script is
being downloaded from [copy tftp://192.168.100.1/poap.py bootflash:scripts/script.sh vrf default ] 2026 Sep 22 18:24:15 switch %$ VDC-1 %$
%POAP-2-POAP_SCRIPT_DOWNLOADED: [FDO262921L3-88:FC:5D:BA:D7:7F] - Successfully downloaded POAP script file
```

Ces messages confirment que le commutateur a récupéré poap.py à partir du serveur TFTP découvert via DHCP.

Vérification de la récupération des scripts avec une capture de paquets

Une capture de paquets fournit une confirmation directe des requêtes TFTP générées pendant l'exécution du script.

Pour l'exemple validé, exécutez :

```
sudo tcpdump -nn -r /tmp/poap-run1.pcap 'udp dst port 69' reading from file /tmp/poap-run1.pcap, link-type EN10MB (Ethernet), snapshot
length 262144 13:38:17.012862 IP 192.168.100.108.58485 > 192.168.100.1.69: TFTP, length 16, RRQ "poap.py" octet 13:38:19.955108 IP
192.168.100.108.58550 > 192.168.100.1.69: TFTP, length 29, RRQ "conf.FDO262921L3.md5" octet 13:38:20.651491 IP
192.168.100.108.58680 > 192.168.100.1.69: TFTP, length 25, RRQ "conf.FDO262921L3" octet 13:38:21.737101 IP 192.168.100.108.58866 >
192.168.100.1.69: TFTP, length 35, RRQ "nxos64-cs.10.6.2.F.bin.md5" octet
```

La première demande confirme que l'adresse POAP temporaire 192.168.100.108 a contacté le serveur d'approvisionnement à l'adresse 192.168.100.1 et a demandé poap.py. Les demandes suivantes montrent la progression vers la configuration des périphériques et la validation des images.

Vérification de l'intégrité du script POAP

Avant l'exécution du script téléchargé, Cisco NX-OS valide la somme de contrôle MD5 intégrée au script.

L'exemple validé produit :

```
2026 Sep 22 18:24:15 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO262921L3-88:FC:5D:BA:D7:7F] - Script file size 113107, MD5
checksum e4dd91fd4296d40abd2f6187152cd86e 2026 Sep 22 18:24:15 switch %$ VDC-1 %$ %POAP-2-POAP_INFO: [FDO262921L3-
88:FC:5D:BA:D7:7F] - MD5 checksum received from the script file is e4dd91fd4296d40abd2f6187152cd86e 2026 Sep 22 18:24:15 switch %$
VDC-1 %$ %POAP-2-POAP_SCRIPT_STARTED_MD5_VALIDATED: [FDO262921L3-88:FC:5D:BA:D7:7F] - POAP script execution
started(MD5 validated)
```

Les valeurs correspondantes confirment que le script téléchargé a réussi le contrôle d'intégrité avant le début de l'exécution.

À ce stade, le contrôle passe de l'initialisation POAP à la logique d'approvisionnement contenue dans le script téléchargé.

Vérification de la récupération de la configuration spécifique au périphérique

Une fois le script POAP démarré, vérifiez qu'il identifie le commutateur Nexus et sélectionne la configuration de périphérique correspondante.

En mode `serial_number`, le script de référence utilise le numéro de série du commutateur local afin de déterminer le nom du fichier de configuration.

L'exemple validé généré :

Définition du nom de fichier source `cfg` en fonction du numéro de série
numéro de série `FDO262921L3`
Nom du fichier de configuration sélectionné : `conf.FDO262921L3`

Le résultat confirme que le script a identifié le numéro de série local et sélectionné `conf.FDO262921L3`.

Vérification de la récupération des fichiers de configuration

Une fois le nom du fichier de configuration sélectionné, le script récupère les informations MD5 correspondantes :

```
2026 Sep 22 18:24:17 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: - Logfile name: /bootflash/20260922182417_poap_23243_script.log -
script.sh 2026 Sep 22 18:24:17 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: - Found 1 POAP script logs - script.sh 2026 Sep 22 18:24:17
```

switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG: - Setting source cfg filename based-on serial number - script.sh 2026 Sep 22 18:24:17
switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG: - serial number FDO262921L3 - script.sh 2026 Sep 22 18:24:17 switch %\$ VDC-1 %\$
%USER-1-SYSTEM_MSG: - Selected conf file name : conf.FDO262921L3 - script.sh 2026 Sep 22 18:24:17 switch %\$ VDC-1 %\$ %USER-1-
SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - Verifying freespace in bootflash - script.sh 2026 Sep 22 18:24:17 switch
%\$ VDC-1 %\$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - Free bootflash space is 106776296.0 KB -
script.sh 2026 Sep 22 18:24:17 switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - Single
image is set - script.sh 2026 Sep 22 18:24:17 switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-
MAC[88:FC:5D:BA:D7:7F] - Copying config file - script.sh 2026 Sep 22 18:24:17 switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG:
S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - Copying MD5 information - script.sh 2026 Sep 22 18:24:17 switch %\$ VDC-1 %\$
%USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - Starting Copy of MD5. src=/conf.FDO262921L3.md5 dest =
/bootflash/conf.FDO262921L3.md5 - script.sh 2026 Sep 22 18:24:17 switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-
MAC[88:FC:5D:BA:D7:7F] - File transfer_protocol = tftp - script.sh

Le fichier d'intégrité est téléchargé et stocké dans la mémoire flash de démarrage : 2026 Sep 22 18:24:17
switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - *** Downloaded file is of size 51 *** -
script.sh 2026 Sep 22 18:24:17 switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] -
Renamed /bootflash/conf.FDO262921L3.md5.tmp to /bootflash/conf.FDO262921L3.md5 - script.sh

Le script récupère ensuite la configuration du périphérique :

2026 Sep 22 18:24:17 switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - INFO: Starting
Copy of Config File to /bootflash/poap_conf.cfg - script.sh 2026 Sep 22 18:24:17 switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG:
S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - Copying file options source=/conf.FDO262921L3 destination=/bootflash/poap_conf.cfg
login_timeout=120 destination_tmp=poap_conf.cfg.tmp - script.sh 2026 Sep 22 18:24:17 switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG:
S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - Transferring using tftp from /conf.FDO262921L3 to bootflash:/poap_conf.cfg.tmp hostname
192.168.100.1 vrf default - script.sh 2026 Sep 22 18:24:17 switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-
MAC[88:FC:5D:BA:D7:7F] - Command is : terminal dont-ask ; terminal password

; copy tftp://root@192.168.100.1/conf.FDO262921L3 bootflash:/poap_conf.cfg.tmp vrf default - script.sh 2026 Sep 22 18:24:18 switch %\$
VDC-1 %\$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - *** Downloaded file is of size 120 *** - script.sh

Ces messages confirment que la configuration spécifique au périphérique a été correctement récupérée et stockée localement pour traitement.

Vérification de la récupération de configuration avec une capture de paquets

La capture de paquets fournit une confirmation indépendante des requêtes TFTP générées par le commutateur Nexus.

Pour l'exemple validé :

```
sudo tcpdump -nn -r /tmp/poap-run1.pcap 'udp dst port 69' reading from file /tmp/poap-run1.pcap, link-type EN10MB (Ethernet), snapshot length 262144 13:38:19.955108 IP 192.168.100.108.58550 > 192.168.100.1.69: TFTP, length 29, RRQ "conf.FDO262921L3.md5" octet 13:38:20.651491 IP 192.168.100.108.58680 > 192.168.100.1.69: TFTP, length 25, RRQ "conf.FDO262921L3" octet
```

La séquence confirme que le commutateur a demandé le fichier d'intégrité de la configuration avant de récupérer la configuration du périphérique.

Le journal du serveur TFTP a également enregistré les deux transferts :

```
Sep 22 14:26:36 calo-ubuntu24-00505692aeaf dnsmasq-tftp[144902]: sent /srv/tftp/conf.FDO262921L3.md5 to 192.168.100.108 Sep 22 14:26:37 calo-ubuntu24-00505692aeaf dnsmasq-tftp[144902]: sent /srv/tftp/conf.FDO262921L3 to 192.168.100.108
```

Vérifier l'intégrité de configuration

Une fois la configuration téléchargée, le script calcule sa somme de contrôle MD5 et la compare à la valeur attendue.

La tentative de mise en service illustrée dans cet exemple a produit :

```
2026 Sep 22 18:24:18 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - Verifying MD5 checksum - script.sh 2026 Sep 22 18:24:18 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - file name is bootflash:poap_conf.cfg - script.sh 2026 Sep 22 18:24:18 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - INFO: md5sum a1a51058d79de0348c6cd1934e08acb4 (recalculated) - script.sh 2026 Sep 22 18:24:18 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - Verifying MD5 checksum of /bootflash/poap_conf.cfg (size 120) - script.sh 2026 Sep 22 18:24:18 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - md5given = a1a51058d79de0348c6cd1934e08acb4 md5calculated = a1a51058d79de0348c6cd1934e08acb4 - script.sh 2026 Sep 22 18:24:18 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - MD5 match for file = /bootflash/poap_conf.cfg - script.sh
```

Les valeurs correspondantes confirment que la configuration téléchargée lors de cette tentative de mise en service correspondait aux informations d'intégrité correspondantes.

Vérification du traitement de configuration

Une fois le contrôle d'intégrité terminé, le script détermine la manière dont la configuration doit être préparée pour l'image cible de Cisco NX-OS.

Dans cet exemple :

```
026 Sep 22 18:24:18 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - Split Config file - script.sh
2026 Sep 22 18:24:18 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - Target image supports bootstrap replay. Split config is not required. - script.sh
2026 Sep 22 18:24:18 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - Skip split config as it isn't needed with nxos64-cs.10.6.2.F.bin - script.sh
```

Le résultat confirme que l'image cible prend en charge la relecture des données d'amorçage et que le fractionnement de la configuration n'est pas nécessaire pour cette tentative d'approvisionnement.

À ce stade, la configuration spécifique au périphérique a été identifiée, récupérée, validée et préparée pour le flux de travail POAP restant.

Vérification du traitement des images

Une fois la configuration du périphérique récupérée et validée, vérifiez comment le script POAP traite l'image Cisco NX-OS cible.

L'implémentation validée utilise : nxos64-cs.10.6.2.F.bin

Le script récupère d'abord les informations MD5 correspondantes :

```
2026 Sep 22 18:24:18 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - Starting Copy of MD5. src=/nxos64-cs.10.6.2.F.bin.md5 dest = /bootflash/nxos64-cs.10.6.2.F.bin.md5 - script.sh
2026 Sep 22 18:24:18 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - File transfer_protocol = tftp - script.sh
```

Le fichier MD5 est ensuite stocké dans la mémoire flash de démarrage :

```
2026 Sep 22 18:24:19 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - *** Downloaded file is of size 57 *** - script.sh
2026 Sep 22 18:24:19 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - Renamed /bootflash/nxos64-cs.10.6.2.F.bin.md5.tmp to /bootflash/nxos64-cs.10.6.2.F.bin.md5 - script.sh
```

Le script lit la somme de contrôle reçue du serveur d'approvisionnement :

2026 Sep 22 18:24:19 switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - MD5 for system image from server: ce50c3f0e387bee578e615a373a4ede0 - script.sh

Il calcule ensuite la somme de contrôle de l'image déjà présente dans le bootflash :

2026 Sep 22 18:24:19 switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - Verifying MD5 checksum - script.sh 2026 Sep 22 18:24:19 switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - file name is bootflash:nxos64-cs.10.6.2.F.bin - script.sh 2026 Sep 22 18:24:30 switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - INFO: md5sum ce50c3f0e387bee578e615a373a4ede0 (recalculated) - script.sh 2026 Sep 22 18:24:30 switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - Verifying MD5 checksum of /bootflash/nxos64-cs.10.6.2.F.bin (size 2952914432) - script.sh 2026 Sep 22 18:24:30 switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - md5given = ce50c3f0e387bee578e615a373a4ede0 md5calculated = ce50c3f0e387bee578e615a373a4ede0 - script.sh

Le script confirme que l'image existante correspond à l'image attendue :

2026 Sep 22 18:24:30 switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - MD5 match for file = /bootflash/nxos64-cs.10.6.2.F.bin - script.sh 2026 Sep 22 18:24:30 switch %\$ VDC-1 %\$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - File /bootflash/nxos64-cs.10.6.2.F.bin already exists and MD5 matches - script.sh

Les valeurs correspondantes confirment que l'image Cisco NX-OS requise était déjà présente dans le bootflash : et a réussi le contrôle d'intégrité. Par conséquent, il n'était pas nécessaire de télécharger une autre copie de l'image.

Vérification de la récupération MD5 de l'image

La capture de paquets confirme également que le Nexus a demandé le fichier d'intégrité d'image :

sudo tcpdump -nn -r /tmp/poap-run1.pcap 'udp dst port 69' reading from file /tmp/poap-run1.pcap, link-type EN10MB (Ethernet), snapshot length 262144 13:38:21.737101 IP 192.168.100.108.58866 > 192.168.100.1.69: TFTP, length 35, RRQ "nxos64-cs.10.6.2.F.bin.md5" octet

Le journal du serveur TFTP a enregistré le même transfert :

Sep 22 14:26:38 calo-ubuntu24-00505692aeaf dnsmasq-tftp[144902]: sent /srv/tftp/nxos64-cs.10.6.2.F.bin.md5 to 192.168.100.108

Ces résultats confirment la récupération de nxos64-cs.10.6.2.F.bin.md5 à partir du serveur d'approvisionnement.

Vérification du workflow d'installation du logiciel

Bien que le fichier image n'ait pas besoin d'être téléchargé, le script de référence a continué avec le workflow d'installation de Cisco NX-OS.

L'exemple validé généré :

```
2026 Sep 22 18:24:31 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-MAC[88:FC:5D:BA:D7:7F] - Done copying the
second scheduled cfg - script.sh 2026 Sep 22 18:24:31 switch %$ VDC-1 %$ %USER-1-SYSTEM_MSG: S/N[FDO262921L3]-
MAC[88:FC:5D:BA:D7:7F] - terminal dont-ask ; install all nxos bootflash:/nxos64-cs.10.6.2.F.bin no-reload non-interruptive - script.sh
```

L'image existante a réussi le contrôle d'intégrité et n'a pas nécessité un autre transfert de fichier. Cependant, le script de référence a toujours appelé le processus d'installation du logiciel par rapport à l'image validée.



Remarque : Une image existante et un MD5 correspondant peuvent empêcher un téléchargement d'image inutile. Cela ne signifie pas nécessairement que le workflow d'installation de logiciel restant est ignoré.

Une fois le traitement logiciel terminé, le POAP poursuit les opérations de provisionnement restantes et prépare le commutateur pour le rechargement.

Vérifier la relecture de configuration

Une fois le script POAP terminé avec succès, vérifiez que le commutateur poursuit le processus de rechargement et de relecture de la configuration.

L'exemple validé signale une exécution réussie du script, puis un rechargement :

```
2026 Sep 22 18:31:08 switch %$ VDC-1 %$ %POAP-2-POAP_SCRIPT_EXEC_SUCCESS: [FDO262921L3-88:FC:5D:BA:D7:7F] - POAP
script execution success 2026 Sep 22 18:31:09 switch %$ VDC-1 %$ %POAP-2-POAP_RELOAD_DEVICE: [FDO262921L3-
88:FC:5D:BA:D7:7F] - Reload device
```

Ces messages confirment l'achèvement de la phase d'exécution du script et la transition vers la phase de rechargement post-installation.

Après le redémarrage du commutateur, Cisco NX-OS détecte le fichier de relecture POAP :

```
2026 Sep 22 18:33:49 %$ VDC-1 %$ %DAEMON-2-SYSTEM_MSG: <<%ASCII-CFG-2-CONF_CONTROL>> Poap replay
/bootflash/poap_replay01.cfg - ascii_cfg_server[17165]
```

La relecture du bootstrap a ensuite démarré et s'est terminée :

```
2026 Sep 22 18:34:26 %$ VDC-1 %$ %ASCII-CFG-2-CONFIG_REPLAY_STATUS: Bootstrap Replay Started. 2026 Sep 22 18:34:27 %$
VDC-1 %$ %ASCII-CFG-2-CONFIG_REPLAY_STATUS: Bootstrap Replay Done.
```

Ces événements confirment que Cisco NX-OS a commencé à traiter la configuration préparée au cours du POAP.

Vérification de la relecture de la configuration ASCII

Une fois la réexécution du bootstrap terminée, NX-OS traite la configuration provisionnée.

Les tentatives de validation contrôlées ont généré les messages suivants :

```
2026 Sep 22 18:35:42 switch %$ VDC-1 %$ %ASCII-CFG-2-CONFIG_REPLAY_STATUS: Ascii Replay Started. 2026 Sep 22 18:35:44
N9K-POAP-SW1 %$ VDC-1 %$ %ASCII-CFG-2-CONFIG_REPLAY_STATUS: Ascii Replay Done. 2026 Sep 22 20:03:26 switch
%VDC_MGR-5-VDC_HOSTNAME_CHANGE: vdc 1 hostname changed to N9K-POAP-SW1 2026 Sep 22 20:03:27 N9K-POAP-SW1
%ETHPORT-5-IF_UP: Interface loopback100 is up 2026 Sep 22 20:03:28 N9K-POAP-SW1 %ASCII-CFG-2-CONFIG_REPLAY_STATUS:
Ascii Replay Done. 2026 Sep 22 20:03:29 N9K-POAP-SW1 %ASCII-CFG-2-CONF_CONTROL: System ready
```

Les messages montrent la réexécution de la configuration ASCII et fournissent une preuve directe que la configuration provisionnée a été appliquée.

Le nom d'hôte est devenu N9K-POAP-SW1 et le bouclage 100 est devenu opérationnel dans le cadre de la configuration provisionnée.

Vérifier la fin du POAP

Une fois la réexécution de la configuration terminée, Cisco NX-OS enregistre la configuration résultante.

```
2026 Sep 22 19:24:03 N9K-POAP-SW1 %$ VDC-1 %$ %ASCII-CFG-2-CONF_CONTROL: System ready
[#####] 100% Copy complete, now saving to disk (please wait)... Copy complete. Auto provisioning
complete
```

Le message Auto provisioning complete (Fin du provisionnement automatique) confirme la fin du workflow POAP.

À ce stade, vérifiez la configuration en cours et la configuration initiale résultantes afin de confirmer que la configuration Day-0 prévue est active et persistante.

Vérification de la configuration provisionnée

Une fois le POAP terminé, vérifiez que la configuration Day-0 prévue est active et persistante. Confirmez le nom d'hôte, le compte d'administration, la configuration d'interface, l'image Cisco NX-OS et l'état POAP du système.

```
N9K-POAP-SW1# show hostname N9K-POAP-SW1 N9K-POAP-SW1# show user-account admin user:admin this user account has no expiry
date roles:network-admin N9K-POAP-SW1# show ip interface brief IP Interface Status for VRF "default"(1) Interface IP Address Interface
Status Lo100 10.255.255.100 protocol-up/link-up/admin-up N9K-POAP-SW1# show running-config interface loopback100 !Command: show
running-config interface loopback100 !Running configuration last done at: Tue Sep 22 20:03:48 2026 !Time: Tue Sep 22 23:17:52 2026 version
10.6(2) Bios:version 05.53 interface loopback100 description POAP-VALIDATION ip address 10.255.255.100/32 N9K-POAP-SW1# show
startup-config interface loopback100 !Command: show startup-config interface loopback100 !Time: Tue Sep 22 23:17:57 2026 !Startup config
saved at: Tue Sep 22 20:03:48 2026 version 10.6(2) Bios:version 05.53 interface loopback100 description POAP-VALIDATION ip address
10.255.255.100/32 N9K-POAP-SW1# show startup-config | include username username admin password 5

role network-admin N9K-POAP-SW1# show version | include NXOS NXOS: version 10.6(2) [Feature Release] Host NXOS: version
10.6(2) NXOS image file is: bootflash:///nxos64-cs.10.6.2.F.bin NXOS compile time: 11/30/2025 12:00:00 [12/12/2025 12:10:23] NXOS boot
mode: LXC N9K-POAP-SW1# show system poap System-wide POAP is enabled
```

Le résultat confirme que la configuration spécifique au périphérique a été correctement appliquée et enregistrée dans la configuration initiale.

Il confirme également que le commutateur exécute l'image Cisco NX-OS attendue et que le protocole POAP à l'échelle du système reste activé.

Conclusion

Ce document décrit les principaux composants et flux de travail POAP, y compris la découverte DHCP, la récupération et l'exécution de scripts, la sélection de configuration spécifique au périphérique, la validation de l'intégrité des fichiers, le traitement des images Cisco NX-OS et la relecture de la configuration.

La mise en oeuvre validée montre comment un commutateur Cisco Nexus 9000 peut obtenir les ressources de mise en service requises, appliquer une configuration de type « Day-0 » et conserver la configuration résultante.

Le processus de vérification montre également comment les messages de console, les journaux POAP, les journaux de serveur et les captures de paquets peuvent être corrélés afin de confirmer chaque étape majeure du workflow de mise en service.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.